3-15-2010

Quantum Information Encoding, Protection, and Correction from Trace-Norm Isometries

Francesco Ticozzi
Universita di Pado

Lorenza Viola
Dartmouth College

Quantum Information Encoding, Protection, and Correction from Trace-Norm Isometries

Francesco Ticozzi*
Dipartimento di Ingegneria dell'Informazione, Università di Padova, via Gradenigo 6/B, 35131 Padova, Italy

Lorenza Viola†
Department of Physics and Astronomy, Dartmouth College, 6127 Wilder Laboratory, Hanover, NH 03755, USA

(Dated: November 5, 2018)

We introduce the notion of trace-norm isometric encoding and explore its implications for passive and active methods to protect quantum information against errors. Beside providing an operational foundations to the "subsystems principle" [E. Knill, Phys. Rev. A **74**, 042301 (2006)] for faithfully realizing quantum information in physical systems, our approach allows additional explicit connections between noiseless, protectable, and correctable quantum codes to be identified. Robustness properties of isometric encodings against imperfect initialization and/or deviations from the intended error models are also analyzed.

PACS numbers: 03.67.Pp, 03.65.Yz, 03.67.Lx, 89.70.-a

I. INTRODUCTION

The idea that states of ideal quantum systems, carrying abstractly defined quantum information, must be suitably mapped – *encoded* – into states of a physical system, in such a way that information can be best protected against the unavoidable effect of errors, underpins the possibility to practically exploit the added power of quantum information in real-world devices. According to the so-called *subsystems principle* [1, 2, 3, 4], logically mapping quantum information into a subsystem of a Hilbert space provides the most general approach to quantum encoding, and well-identifiable subsystems must exist at each point in time in order for the desired information to be faithfully represented throughout a computational process. Subsystem-encodings play a central role in the theory of quantum fault tolerance, allowing, in particular, for a unified understanding of quantum error control to be gained in terms of passive protection based on decoherence-free subspaces [5, 6] and noiseless subsystems [2], as well as active stabilization based on either "initialization-protectable" or "error-correcting subsystems" [4]. Conceptually, the subsystems principle provides the foundation for operator quantum error correction (OQEC) [7, 8, 9], which is the most general error-control framework presently known for noise described by a completely positive trace-preserving (CPTP) map.

For physically realized information, recent work by Blume-Kohout and coworkers [10, 11] has shown that preservation of the *mutual distinguishability* between states under a given error process is key to a general *operational* characterization of the information-preserving structures (IPS) that the process can support, whether in passive or active form. Mathematically, the starting point is to realize that preservation of information in a set of possible states (a *code*) under the action of a map $\mathcal{E}$ is equivalent to requiring that $\mathcal{E}$ acts on the code as a distance-preserving map, where the appropriate distance measure is induced by the *trace norm*. Remarkably, since the latter yields both lower and upper bound to the fidelity between quantum states [12], the trace norm provides the appropriate metric of performance for quantifying distance between open-system evolutions [13, 14].

In the light of the special significance that both subsystems and trace-norm isometries have in the broad QEC context, a natural question arises: Can these notions be related at a fundamental level? Equivalently, *what role do trace-norm isometries play in representing quantum information?* Exploring the implications of a description that directly exploits trace-norm isometries is the main motivation of this work. We show that by insisting in the requirement that quantum information encodings be 1-isometries, a number of *a priori* unrelated results are consistently recovered, and additional new insight is gained. In particular, our first result (Sec. II) is the possibility to *derive* a manifestation of the subsystems principle, thereby firmly grounding it on operational requirements. In Sec. III, an explicit form of the most general codes that can faithfully encode quantum information and of the class of transformations that preserve and recover these codes is obtained. In the process, we elucidate connections between the dual notions of *correctability* and *protectability* that were not captured by the previous IPS analysis [10], and further characterize QEC scenarios whereby the required active intervention may be achieved through purely unitary means [15, 16]. In Sec. IV, we argue that the trace-norm isometric approach developed for describing perfect quantum information encoding and recovery may serve as a useful starting point for investigating 'perturbations' around exact notions, thus complementing ongoing investigations of *approximate* QEC [17, 18, 19, 20]. We conclude in Sec. V with some open questions.

*Electronic address: ticozzi@dei.unipd.it
†Electronic address: lorenza.viola@dartmouth.edu

II. QUANTUM INFORMATION ENCODINGS

Consider an ideal quantum system $\mathcal{Q}$, defined on a Hilbert space $\mathcal{H}_\mathcal{Q}$, with states belonging to the trace-one, positive, convex subset $\mathcal{D}(\mathcal{H}_\mathcal{Q})$ of the Hermitian operators $\mathcal{O}(\mathcal{H}_\mathcal{Q})$, representing physical observables. $\mathcal{Q}$ represents the *logical* level, the abstract quantum information to be encoded. Our task is to represent quantum information carried by $\mathcal{Q}$ in a given quantum *physical* system $\mathcal{P}$, defined on a Hilbert space $\mathcal{H}_\mathcal{P}$, with corresponding states $\mathcal{D}(\mathcal{H}_\mathcal{P})$ and observables $\mathcal{O}(\mathcal{H}_\mathcal{P})$.

An *encoding* of $\mathcal{Q}$ in $\mathcal{P}$ is specified once two maps, a *state encoding* Φ and an *observable encoding* Ψ, are given:

$$\Phi : \mathcal{D}(\mathcal{H}_\mathcal{Q}) \to \Sigma, \tag{1}$$

$$\Psi : \mathcal{O}(\mathcal{H}_\mathcal{Q}) \to \Omega, \tag{2}$$

where the elements of Σ and Ω are nonempty sets of $\mathcal{D}(\mathcal{H}_\mathcal{P})$ and $\mathcal{O}(\mathcal{H}_\mathcal{P})$, respectively. The use of subsets instead of single operators allows for the possibility that the encoding is insensitive (robust) against the choice of a 'co-subsystem' state, as it will be clear shortly (see discussion after Theorem 1).

In Ref. 4, Knill has formalized the meaning of a *faithful* encoding, by requiring that the encoding maps satisfy three physically-motivated conditions as follows:

(i) Statics: For all $\sigma \in \Phi(\rho)$, $X \in \Psi(A)$, expectation values coincide on faithfully encoded states: $\mathrm{trace}(\sigma X) = \mathrm{trace}(\rho A)$;

(ii) Unitary dynamics: For all $\sigma \in \Phi(\rho)$, $X \in \Psi(A)$, $e^{-iX}\sigma e^{iX} = e^{-iA}\rho e^{iA}$;

(iii) Measurement dynamics: For all $\sigma \in \Phi(\rho)$, $X \in \Psi(A)$, with $X = \sum_\lambda \lambda \Pi_X^\lambda$, $A = \sum_\alpha \alpha \Pi_A^\alpha$ denoting the corresponding spectral representations [21], projective measures are faithfully implemented in the sense that $\Pi_X^\lambda \sigma \Pi_X^\lambda \in \Phi(\Pi_A^\lambda \rho \Pi_A^\lambda)$.

It is then proved (Thm. 1 in [4]) that every *faithful encoding of quantum information is a subsystem encoding*, that is, there exists a decomposition

$$\mathcal{H}_\mathcal{P} = \mathcal{H}_S \otimes \mathcal{H}_F \oplus \mathcal{H}_R, \tag{3}$$

such that for all ρ, $\mathrm{supp}(\Phi(\rho)) \subset \mathcal{H}_S \otimes \mathcal{H}_F$, and for all $X \in \Psi(A)$, $\Psi(A)$ is of the form $X_S \otimes I_F \oplus X_R$. Motivated by the operational requirement of distinguishability preservation between sets of states [10, 11], we now introduce *1-isometric encodings*, and compare them with faithful encodings. In what follows, we shall primarily focus on encoding of states, which is the key for quantum information protection and correction in the Schroedinger's picture.

It is well known [22, 23, 24] that the probability of correctly distinguishing a pair of quantum states is related to the distance induced by the trace-norm,

$$\|A\|_1 \equiv \mathrm{trace}(|A|) = \sum_i s_i(A),$$

where $|A| \equiv \sqrt{A^\dagger A}$ and $s_i(A)$ are the singular values. Specifically, let two states ρ, τ, be prepared with prior probability $p, 1-p$, respectively. Then they can be discriminated by means of measurements with at most probability $\frac{1}{2}(1 + \|p\rho - (1-p)\tau\|_1)$. This naturally prompts investigating the structure of encodings that preserve distinguishability:

Definition 1 *A linear map on Hermitian operators, $\Phi : \mathcal{O}(\mathcal{H}_\mathcal{Q}) \to \mathcal{O}(\mathcal{H}_\mathcal{P})$, defines a 1-isometric encoding if for all $\rho_1, \rho_2 \in \mathcal{D}(\mathcal{H}_\mathcal{Q})$ and $p \in [0,1]$,*

$$\|p\Phi(\rho_1) - (1-p)\Phi(\rho_2)\|_1 = \|p\rho_1 - (1-p)\rho_2\|_1. \tag{4}$$

Notice that linearity is assumed here from the beginning, reflecting the fact that, in practice, any physical procedure to be employed as an information "encoder" can be described as a linear state transformation. While distinguishability preservation might at first seem a weak requirement in comparison with (i)-(iii) for faithful encodings, we shall next show that it is indeed enough to enforce a subsystem structure. We begin with a preliminary Lemma:

Lemma 1 *If Eq.* (4) *holds for any $\rho_1, \rho_2 \in \mathcal{D}(\mathcal{H}_\mathcal{Q})$, the map Φ is a linear isometry on the whole $\mathcal{O}(\mathcal{H}_\mathcal{Q})$.*

Proof. Any $Z \in \mathcal{O}(\mathcal{H}_\mathcal{Q})$ may be expressed in the form

$$Z = Z^+ - Z^- = \mathrm{trace}(Z^+)\rho_+ - \mathrm{trace}(Z^-)\rho_-,$$

where $Z^{+,-}$ are the positive and negative parts of Z, respectively, and $\rho_{+,-} = Z^{+,-}/\mathrm{trace}(Z^{+,-}) \in \mathcal{D}(\mathcal{H}_\mathcal{Q})$. By letting $p = \mathrm{trace}(Z^+)/\mathrm{trace}(Z^+ + Z^-)$, we get

$$\begin{aligned} \|\Phi(Z)\|_1 &= \|\mathrm{trace}(Z^+)\Phi(\rho_+) - \mathrm{trace}(Z^-)\Phi(\rho_-)\|_1 \\ &= (\mathrm{trace}(Z^+ + Z^-))\|p\Phi(\rho_+) - (1-p)\Phi(\rho_-)\|_1 \\ &= (\mathrm{trace}(Z^+ + Z^-))\|p\rho_+ - (1-p)\rho_-\|_1 \\ &= \|\mathrm{trace}(Z^+)\rho_+ - \mathrm{trace}(Z^-)\rho_-\|_1 \\ &= \|Z\|_1. \end{aligned}$$

Thus, Φ is an isometry on $\mathcal{O}(\mathcal{H}_\mathcal{Q})$. □

Since $\Phi : \mathcal{O}(\mathcal{H}_\mathcal{Q}) \to \mathcal{O}(\mathcal{H}_\mathcal{P})$ is a linear 1-isometry that sends states to states, it defines a *stochastic isometry* in the terminology of Busch [25]. By invoking Thm. 1 of Ref. 25, in particular, it follows that for every 1-isometric encoding as defined above, there exists a decomposition of the form

$$\mathcal{H}_\mathcal{P} = \Big(\bigoplus_j \mathcal{H}_{S,j}\Big) \oplus \mathcal{H}_R, \tag{5}$$

with each $\mathcal{H}_{S,j}$ isomorphic to $\mathcal{H}_Q$, such that

$$\Phi(\rho) = \Big(\bigoplus_j \omega_j U_j \rho U_j^\dagger\Big) \oplus \hat{0}_R, \tag{6}$$

where $U_j : \mathcal{H}_\mathcal{Q} \to \mathcal{H}_{S,j}$ is either unitary or anti-unitary, $\omega_j \in [0,1]$, $\sum_j \omega_j = 1$, and $\hat{0}_R$ denotes the zero operator on $\mathcal{H}_R$ (on the topic of isometric mappings between quantum states, see also [26, 27]). Thus, up to a unitary (or anti-unitary) transformation $U_{\mathcal{P}} = \left(\bigoplus_j U_j^\dagger\right) \oplus \hat{I}_R$ on $\mathcal{H}_{\mathcal{P}}$, and a possible reordering of the basis, it follows that *for any 1-isometric state encoding there exists a subsystem decomposition* of $\mathcal{H}_{\mathcal{P}}$ of the form given in Eq. (3), such that

$$\Phi(\rho) = \rho \otimes \tau \oplus \hat{0}_R, \tag{7}$$

with a density operator τ on the co-subsystem factor $\mathcal{H}_F$ with spectrum $\{\omega_j\}$.

We remark that the subsystem decomposition of the Hilbert space $\mathcal{H}_{\mathcal{P}}$ associated to a given encoding Φ is in general *not* unique. In particular, there exists a *minimal* decomposition for which the state τ in (7) is *full-rank* in $\mathcal{H}_F$. The other subsystem decompositions of $\mathcal{H}_{\mathcal{P}}$ may be obtained from the minimal one by augmenting the dimension of $\mathcal{H}_F$ (thus reducing the one of the summand $\mathcal{H}_R$) upon identifying more isomorphic copies of $\mathcal{H}_{S,j} \sim \mathcal{H}_{\mathcal{Q}}$ in (5), associated to weights $\omega_j = 0$ in (6). The latter subspaces do not actually encode any information, since the state has trivial support there.

Once a subsystem decomposition of $\mathcal{H}_{\mathcal{P}}$ is chosen, a natural observable encoding Ψ is given by

$$\Psi(A) = A \otimes I_F \oplus X_R, \tag{8}$$

for some $X_R \in \mathcal{O}(\mathcal{H}_R)$ [28]. Given the structure of the encoded states in Eq. (7), the specific choice of non-minimal subsystem decomposition and of X_R is irrelevant for expectations, dynamics, and measurement on the encoded states. In fact, one may directly verify that any pair (Φ, Ψ) of the form given in Eqs. (7)-(8) defines a faithful encoding, and that the requirements (i)-(iii) do not depend on the co-factor state, τ. Conversely, consider a faithful encoding $(\bar{\Phi}, \bar{\Psi})$. Then the associated subsystem structure provides us with a class of 1-isometric state encodings Φ_τ as in Eq. (7), parametrized by the state of the co-factor $\tau \in \mathcal{D}(\mathcal{H}_F)$. Each pair $(\Phi_\tau, \bar{\Psi})$ is a faithful encoding. We can summarize these properties in the following:

Theorem 1 *To every 1-isometric encoding Φ is associated a (minimal) faithful subsystem encoding of the form given in Eqs. (7)–(8), and to every faithful encoding $(\bar{\Phi}, \bar{\Psi})$ is associated a class of 1-isometric encodings Φ_τ parametrized by the co-factor state $\tau \in \mathcal{D}(\mathcal{H}_F)$.*

This result provides an explicit connection between 1-isometric and faithful encodings. In fact, Thm. 1 may be regarded as establishing a *subsystems principle* building on the operational notion of distinguishability.

By requiring the state encoding Φ to be a *linear and isometric* function, we lose in principle some of the structure associated with the general encoding maps of [4] into *subsets*, Eqs. (1)–(2). Nonetheless, it is important to appreciate that to each subsystem decomposition is associated a *class* of isometric encodings, parametrized by the cofactor state τ. The latter are operationally indistinguishable with respect to the faithfulness requirements (i)-(iii), as long as they they share the same observable encoding of the form (8). One can then think to describe such a class in a compact form as a state encoding into subsets:

$$\hat{\Phi} : \rho \in \mathcal{D}(\mathcal{H}_{\mathcal{Q}}) \mapsto \Sigma_\rho = \{\rho \otimes \tau \oplus \hat{0}_R | \tau \in \mathcal{D}(\mathcal{H}_{\mathcal{F}})\}.$$

When the observable encoding is defined as in (8), $\hat{\Phi}$ can be interpreted as a *robust* encoding with respect to τ, in the sense that the desired information is correctly represented in $\mathcal{H}_S$ irrespective of which element of Σ_ρ has been used. Such a robustness property plays a crucial role for characterizing the potential of error correction and protection of 1-isometric quantum codes, to which we turn next.

III. NOISELESS, PROTECTABLE, AND CORRECTABLE CODES

Consider a 1-isometric encoding (Φ, Ψ) of $\mathcal{Q}$ in $\mathcal{P}$: We shall henceforth denote $\Phi(\mathcal{D}(\mathcal{H}_{\mathcal{Q}}))$ by $\mathcal{C}_{\mathcal{Q}}$ and call it a *code*. Assume that as a result of some noise process, the physical system $\mathcal{P}$ undergoes CPTP dynamics described by a quantum operation $\mathcal{E}$ on $\mathcal{D}(\mathcal{H}_{\mathcal{P}})$. We start by recalling three desirable properties that $\mathcal{C}_{\mathcal{Q}}$ may exhibit with respect to $\mathcal{E}$, following the definitions given in Blume-Kohout *et al.* [10]:

Definition 2 *A code $\mathcal{C}_{\mathcal{Q}}$ is (i)* fixed *by $\mathcal{E}$ if $\mathcal{E}(\rho) = \rho$ for every $\rho \in \mathcal{C}_{\mathcal{Q}}$; (ii)* preserved *by $\mathcal{E}$ if $\mathcal{E}$ acts as a 1-isometry on $\mathcal{C}_{\mathcal{Q}}$; (iii)* noiseless *for $\mathcal{E}$ if it is preserved by any convex mixture $\sum_k p_k \mathcal{E}^k$, with $p_k \geq 0$ and $\sum_k p_k = 1$.*

Our focus in this Section is to study in detail how, within the present 1-isometric framework, the above properties relate to both passive and active methods for stabilizing information encoded in $\mathcal{C}_{\mathcal{Q}}$ against $\mathcal{E}$.

A. Noiseless isometric codes and subsystems

The noiselessness property as stated in Definition 2 appears at first quite different from the original concept underlying decoherence-free subspaces (DFSs) [5, 6] and, more generally, noiseless subsystems (NSs) [2, 3, 4, 29]. While a number of equivalent characterizations exist, the following may be taken as the standard defining property of a NS: Given a fixed decomposition of the Hilbert space, $\mathcal{H}_{\mathcal{P}} = \mathcal{H}_S \otimes \mathcal{H}_F \oplus \mathcal{H}_R$, and a TPCP $\mathcal{E}$, $\mathcal{H}_S$ supports a NS for $\mathcal{E}$ if for every $\rho_S \in \mathcal{D}(\mathcal{H}_S)$, $\tau_F \in \mathcal{D}(\mathcal{H}_F)$,

$$\mathcal{E}(\rho_S \otimes \tau_F) = \rho_S \otimes \sigma_F, \tag{9}$$

for some state $\sigma_F \in \mathcal{D}(\mathcal{H}_F)$. That is, the restriction of $\mathcal{E}$ to $\mathcal{H}_S \otimes \mathcal{H}_F$ obeys

$$\mathcal{E}|_{\mathcal{H}_S \otimes \mathcal{H}_F} = I_S \otimes \mathcal{F}, \tag{10}$$

for some TPCP $\mathcal{F}$ on $\mathcal{H}_F$.

From Eq. (9), it is easy to show that a noiseless 1-isometric code exists with support on the same factor $\mathcal{H}_S$. In fact, it suffices to consider a state $\tau \in \mathcal{D}(\mathcal{H}_\mathcal{F})$ which is a fixed point for $\mathcal{F}$, and observe that the code $\rho \otimes \tau \oplus \hat{0}_R$ is fixed for $\mathcal{E}$, and hence it is trivially noiseless. The converse is not equally straightforward: *Given that a TPCP map admits a noiseless 1-isometric code, is there a noiseless subsystem that shares the same (or a compatible) subsystem structure?*

The rest of this section is devoted to prove that this is indeed the case. We begin with the following Lemma:

Lemma 2 *Let $\mathcal{E} : \mathcal{D}(\mathcal{H}_\mathcal{P}) \rightarrow \mathcal{D}(\mathcal{H}_\mathcal{P})$ be a TPCP map and $\bar{\rho} \in \mathcal{D}(\mathcal{H}_\mathcal{P})$ such that $\mathcal{E}(\bar{\rho}) = \bar{\sigma}$, with $supp(\bar{\sigma}) \subseteq supp(\bar{\rho})$. Let $\mathcal{D}(\bar{\mathcal{H}})$ be the set of density operators with support only on $\bar{\mathcal{H}} = \mathrm{supp}(\bar{\rho})$. Then $\mathcal{E}(\mathcal{D}(\bar{\mathcal{H}})) \subset \mathcal{D}(\bar{\mathcal{H}})$.*

Proof. Let us choose an operator-sum representation $\mathcal{E}(\cdot) = \sum_k M_k \cdot M_k^\dagger$. Consider the orthogonal decomposition $\mathcal{H}_\mathcal{P} = \bar{\mathcal{H}} \oplus \bar{\mathcal{H}}^\perp$: In a block-matrix representation consistent with such a decomposition, we may write

$$\bar{\rho} = \left(\begin{array}{c|c} \rho_S & 0 \\ \hline 0 & 0 \end{array} \right), \quad M_k = \left(\begin{array}{c|c} M_{k,S} & M_{k,P} \\ \hline M_{k,Q} & M_{k,R} \end{array} \right),$$

$$\mathcal{E}(\bar{\rho}) = \left(\begin{array}{c|c} * & * \\ \hline * & \sum_k M_{Q,k}\rho_S M_{Q,k}^\dagger \end{array} \right) = \bar{\sigma}, \quad \bar{\sigma} = \left(\begin{array}{c|c} \sigma_S & 0 \\ \hline 0 & 0 \end{array} \right).$$

Then it must be $\sum_k M_{Q,k}\rho_S M_{Q,k}^\dagger = 0$, and since ρ_S is full-rank on $\bar{\mathcal{H}}$, this implies $M_{Q,k} = 0$ for all k. It is then easy to verify that this ensures $\mathcal{E}(\mathcal{D}(\bar{\mathcal{H}})) \subseteq \mathcal{D}(\bar{\mathcal{H}})$. □

By using the previous Lemma, we first show that if the action of the map respects a fixed Hilbert space decomposition, the link between noiseless isometric codes and NSs can be established directly:

Theorem 2 *Consider a fixed Hilbert space decomposition $\mathcal{H}_\mathcal{P} = \mathcal{H}_S \otimes \mathcal{H}_F \oplus \mathcal{H}_R$ and a TPCP map $\mathcal{E} : \mathcal{D}(\mathcal{H}_\mathcal{P}) \rightarrow \mathcal{D}(\mathcal{H}_\mathcal{P})$. Assume that there exists a full-rank state $\tau \in \mathcal{D}(\mathcal{H}_F)$, such that for every $\rho \in \mathcal{D}(\mathcal{H}_S)$,*

$$\mathcal{E}(\rho \otimes \tau \oplus \hat{0}_R) = \rho \otimes \sigma \oplus \hat{0}_R, \tag{11}$$

for some $\sigma \in \mathcal{D}(\mathcal{H}_F)$. Then

$$\mathcal{E}|_{\mathcal{H}_S \otimes \mathcal{H}_F} = I_S \otimes \mathcal{F}, \tag{12}$$

for some TPCP $\mathcal{F} : \mathcal{D}(\mathcal{H}_F) \rightarrow \mathcal{D}(\mathcal{H}_F)$.

Proof. First consider a full-rank state $\rho \in \mathcal{D}(\mathcal{H}_S)$. Then

$$\mathrm{supp}(\rho \otimes \sigma \oplus \hat{0}_{R'}) \subseteq \mathcal{H}_S \otimes \mathcal{H}_F = \mathrm{supp}(\rho \otimes \tau \oplus \hat{0}_R),$$

and Lemma 2 implies that

$$\mathcal{E}|_{\mathcal{H}_S \otimes \mathcal{H}_F}(\mathcal{D}(\mathcal{H}_S \otimes \mathcal{H}_F)) \subseteq \mathcal{D}(\mathcal{H}_S \otimes \mathcal{H}_F).$$

We can then restrict our attention to $\mathcal{H}_S \otimes \mathcal{H}_F$. Consider an operator-sum representation for $\mathcal{E}|_{\mathcal{H}_S \otimes \mathcal{H}_F}(\cdot) = \sum_k M_k \cdot M_k^\dagger$. Let $\{C_i \otimes D_j\}$ be an orthonormal operator basis for the corresponding operator space $\mathcal{B}(\mathcal{H}_S \otimes \mathcal{H}_F)$, with $C_0 = I_S$. We may thus rewrite

$$M_k = \sum_{i,j} m_{kij} C_i \otimes D_j = \sum_i C_i \otimes F_{ik},$$

with $F_{ki} = \sum_j m_{kij} D_j$. It then follows that

$$\mathcal{E}(\rho \otimes \tau \oplus \hat{0}_R) = \sum_{klm} C_l \rho C_m^\dagger \otimes F_{lk} \tau F_{mk}^\dagger = \rho \otimes \sigma.$$

Since the $\{C_i\}$ are orthonormal, it must be

$$\sum_k C_l \rho C_l^\dagger \otimes F_{lk} \tau F_{lk}^\dagger = 0,$$

for $l > 0$ and all $\rho \in \mathcal{D}(\mathcal{H}_S)$. This implies $\sum_k F_{lk} \tau F_{lk}^\dagger = 0$ and, since τ is full rank by hypothesis, $F_{lk} = 0$ for $l \neq 0$. We thus get the conclusion with $\mathcal{F}(\cdot) = \sum_k F_{0k} \cdot F_{0k}^\dagger$. □

In the general case where the Hilbert space decomposition is allowed to change, the argument is less direct. Building on the above results, we have the following:

Theorem 3 *Let $\mathcal{C} \sim \rho \otimes \sigma \oplus \hat{0}_R$ be a 1-isometric noiseless for $\mathcal{E}$. Then there exists a fixed code $\mathcal{C}' \sim \rho \otimes \tau \oplus \hat{0}_R$ that admits a subsystem decomposition in common with $\mathcal{C}$ and for which, denoting by $\mathcal{H}_{\mathcal{C}'}$ the support of $\mathcal{C}'$, $\mathcal{E}|_{\mathcal{H}_{\mathcal{C}'}} = I_S \otimes \mathcal{F}$.*

Proof. Consider an infinite, convergent series

$$\bar{\mathcal{E}} = \sum_{i=0}^{\infty} p_i \mathcal{E}^i, \quad \sum_{i=0}^{\infty} p_i = 1,\, p_i > 0.$$

Then, any convex combination $\mathcal{G} = \sum_i q_i \mathcal{E}^i$, with $\sum_i q_i = 1$, $q_i \geq 0$, satisfies $\mathrm{supp}(\mathcal{G}(\mathcal{C})) \subseteq \mathrm{supp}(\bar{\mathcal{E}}(\mathcal{C}))$. Define $\mathcal{H}_{SF} \equiv \mathrm{supp}(\bar{\mathcal{E}}(\mathcal{C}))$ and let $\rho \otimes \bar{\tau} \oplus \hat{0}_R$ be a minimal subsystem representation of $\bar{\mathcal{E}}(\mathcal{C})$. Consider an orthonormal basis $\{|\varphi_j\rangle\}$ of $\mathcal{H}_Q$, and the associated orthogonal projections $\Pi_j = |\varphi_j\rangle\langle\varphi_j|$. Define the isomorphic subspaces $\mathcal{H}_{F,j} \equiv \mathrm{supp}(\Pi_j \otimes \bar{\tau})$. By hypothesis, the combination of the encoding and the evolution $\bar{\mathcal{E}} \circ \Phi$ must act like a trace-norm isometry, and trace-norm isometries preserve orthogonality [25]. Thus, by definition of $\bar{\mathcal{E}}$ and orthogonality preservation, it follows that one can define a family of orthogonal subspaces

$$\begin{aligned} \mathcal{H}_{F,j} &= \mathrm{supp}(\bar{\mathcal{E}}(\Pi_j \otimes \sigma)), \;\; \forall j, \\ \mathcal{H}_{F,j} &\perp \mathcal{H}_{F,k},\; j \neq k. \end{aligned}$$

Pick now an orthonormal basis in each $\mathcal{H}_{F,j}$, such that, for instance, $\bar{\mathcal{E}}(\Pi_j \otimes \sigma)$ is diagonal in $\mathcal{H}_{F,j}$. We can then construct a decomposition

$$\mathcal{H}_{SF} = \bigoplus_j \mathcal{H}_{F,j} = \mathcal{H}_S \otimes \mathcal{H}_F \tag{13}$$

Since, by definition of $\bar{\mathcal{E}}$, it must also be $\text{supp}(\mathcal{E}^i(\Pi_j \otimes \sigma)) \subseteq \mathcal{H}_{F,j}$ for any i, the subsystem structure in (13) supports not only $\bar{\mathcal{E}}(\mathcal{C})$, but each $\mathcal{E}^i(\mathcal{C})$ in subsystem form up to a unitary change of basis in each of the $\mathcal{H}_{F,j}$'s. That is,

$$\mathcal{E}^i(\mathcal{C}) \sim U^{(i)}\Big(\rho \otimes \tau(i) \oplus \hat{0}_R\Big)U^{(i)\dagger}$$

on $\mathcal{H}_S \otimes \mathcal{H}_F \oplus \mathcal{H}_R$, with $\mathcal{H}_R = \mathcal{H} \ominus \mathcal{H}_{SF}$ and a block-unitary $U^{(i)} = \bigoplus_j U_j^{(i)} \oplus I_R$ which in general depends on the exponent i of $\mathcal{E}^i$. The same holds for any convex combination of powers of $\mathcal{E}$: In particular, consider the convex combination

$$\mathcal{E}_N = \sum_{i=0}^{N} \frac{1}{N+1}\mathcal{E}^i.$$

Then the limit $\mathcal{E}_\infty = \lim_{N\to\infty} \mathcal{E}_N$ is well defined for finite-dimensional Hilbert spaces. In addition, $\mathcal{E} \circ \mathcal{E}_\infty = \mathcal{E}_\infty$, hence $\mathcal{E}_\infty$ projects onto the fixed points of $\mathcal{E}$ [10, 30]. Furthermore, $\mathcal{C}_\infty \equiv \mathcal{E}_\infty(\mathcal{C})$ must be of the form $\rho \otimes \tau_\infty \oplus \hat{0}_R$ with respect to the decomposition $\mathcal{H}_\mathcal{P} = \mathcal{H}_S \otimes \mathcal{H}_F \oplus \mathcal{H}_R$, after some change of basis $U_\infty = \Big(\bigoplus_j U_{\infty,j}\Big) \oplus I_R$, constructed as described above. It therefore follows that

$$\mathcal{E}(\rho \otimes \tau_\infty \oplus \hat{0}_R) = \rho \otimes \tau_\infty \oplus \hat{0}_R,$$

for all $\rho \in \mathcal{D}(\mathcal{H}_\mathcal{P})$. If we restrict to the support of the code, we can apply Theorem 2, hence it follows that $\mathcal{E}|_{\text{supp}(\mathcal{C}_\infty)} = I_S \otimes \mathcal{F}$. □

B. Correctable vs. protectable codes

When no DFS or NS can be found under the error dynamics induced by $\mathcal{E}$, active intervention via a recovery quantum operation $\mathcal{R}$ is required in order to protect quantum information encoded in $\mathcal{P}$. For a given $\mathcal{R}$, the subsystems principle implies that stored information must exist irrespective of whether active intervention is effected *before* or *after* error events take place, in a suitable sense [2, 4]. This is formalized by the following:

Definition 3 *A code $\mathcal{C}_\mathcal{Q}$ is (i)* correctable *for $\mathcal{E}$ if there exists a CPTP map $\mathcal{R}$ on $\mathcal{D}(\mathcal{H}_\mathcal{P})$ such that $\mathcal{C}_\mathcal{Q}$ is noiseless for $\mathcal{R} \circ \mathcal{E}$; (ii)* protectable *for $\mathcal{E}$ if $\mathcal{C}_\mathcal{Q}$ is noiseless for $\mathcal{E} \circ \mathcal{R}$.*

Two specializations of the above definitions will also be relevant: we shall call *unitarily correctable (protectable)* a code for which $\mathcal{R}$ can be chosen to be a unitary transformation on $\mathcal{H}_\mathcal{P}$ (see also [11, 15]), and *completely correctable (protectable)* a code which is *fixed* for $\mathcal{R} \circ \mathcal{E}$ (or, respectively, $\mathcal{E} \circ \mathcal{R}$).

Note that what we refer to as completely correctable codes directly correspond to the original notion of a (finite-distance) QEC code, in which case the state of the syndrome subsystem (in the language of [31], Thm. III.5) has to be appropriately re-initialized to its reference state at each iteration, and the code subspace effectively forms a DFS under $\mathcal{R} \circ \mathcal{E}$ [31]. NSs and OQEC, on the other hand, require from the outset that the state of the syndrome subsystem be irrelevant as long as information is properly encoded in the logical factor [2, 10, 29]. While OQEC does not lead to fundamentally different quantum codes (in the sense that for each OQEC code, an associated subspace QEC code may be found), simplified recovery procedures may result from taking explicit advantage of the subsystem structure [32]. In the framework of 1-isometric codes, our first result is to show how the correspondence between NSs and noiseless isometric codes highlighted in the previous section is complemented by the following correctability property:

Theorem 4 *A 1-isometric code $\mathcal{C}_\mathcal{Q}$ is preserved iff it is correctable, and it is correctable iff it is completely correctable.*

Proof. Assume that $\mathcal{C}_\mathcal{Q}$, of the form given in Eq. (7), is preserved by $\mathcal{E}$. Hence $\mathcal{E} \circ \Phi$ is a 1-isometry from $\mathcal{D}(\mathcal{H}_\mathcal{Q})$ on $\mathcal{D}(\mathcal{H}_\mathcal{P})$ and, by Theorem 1, $\mathcal{E}(\mathcal{C}_\mathcal{Q})$ must correspond to another subsystem state-encoding of $\mathcal{Q}$ in $\mathcal{P}$. Assume the two subsystem decompositions of $\mathcal{H}_\mathcal{P}$, corresponding to $\mathcal{C}_\mathcal{Q}$ and $\mathcal{E}(\mathcal{C}_\mathcal{Q})$, respectively, to be $\mathcal{H}_S \otimes \mathcal{H}_F \oplus \mathcal{H}_R$ and $\mathcal{H}_{S'} \otimes \mathcal{H}_G \oplus \mathcal{H}_T$, with $\dim(\mathcal{H}_S) = \dim(\mathcal{H}_{S'}) = \dim(\mathcal{H}_\mathcal{Q})$. The action of $\mathcal{E}$ restricted to $\mathcal{C}_\mathcal{Q}$ can be represented in the form

$$\mathcal{E}|_{\mathcal{C}_\mathcal{Q}} = \mathcal{U}_{S-S'} \otimes \mathcal{E}_{F-G},$$

with $\mathcal{U}_{S-S'}$ a unitary map from $\mathcal{D}(\mathcal{H}_S)$ to $\mathcal{D}(\mathcal{H}_{S'})$, and $\mathcal{E}_{F-G}$ a CPTP map from $\mathcal{D}(\mathcal{H}_F)$ to $\mathcal{D}(\mathcal{H}_G)$, respectively. Let $\mathcal{E}_{F-G}(\tau) = \sigma$. Thus, given the definition of a noiseless code given in Definition 2, $\mathcal{C}_\mathcal{Q}$ is corrected by any $\mathcal{R}$ which obeys

$$\mathcal{R}|_{\mathcal{E}(\mathcal{C}_\mathcal{Q})} = \mathcal{U}^\dagger_{S-S'} \otimes \mathcal{R}_{G-F},$$

with $\mathcal{R}_{G-F}(\sigma) = \tau$. One may for instance employ the time-reversal of $\mathcal{E}_{F-G}$ [33, 34]: That is, let $\{E_k\}$ be the Kraus operators associated to $\mathcal{E}_{F-G}$, then its time-reversal with respect to σ is $\mathcal{R}_{\mathcal{E}_{F-G},\sigma}$ with Kraus operators $\{\sigma^{\frac{1}{2}} E_k^\dagger \tau^{-\frac{1}{2}}\}$. Notice that not only does this correction operation make $\mathcal{C}_\mathcal{Q}$ a noiseless code, but actually a code of fixed points.

Conversely, preservation is necessary for correctability since every CPTP map acts like a trace-norm contraction on states (see *e.g.* [24]):

$$\|\mathcal{E}(\rho_1) - \mathcal{E}(\rho_2)\|_1 \leq \|\rho_1 - \rho_2\|_1,\ \forall \rho_1, \rho_2 \in \mathcal{D}(\mathcal{H}_\mathcal{P}). \quad (14)$$

If $\mathcal{C}_\mathcal{Q}$ is not preserved by $\mathcal{E}$, there must exist $\rho_1, \rho_2 \in \mathcal{C}_\mathcal{Q}$ such that $\|\mathcal{E}(\rho_1) - \mathcal{E}(\rho_2)\|_1 < \|\rho_1 - \rho_2\|_1$. To correct those states, any correction $\mathcal{R}$ should violate (14), and hence it would not be a physically realizable TPCP map. □

Remarkably, a similar reasoning allows us to extend the analysis to protectable codes:

Corollary 1 *A TPCP map $\mathcal{E}$ admits a 1-isometric protectable code $\mathcal{C}_\mathcal{Q}$ iff it admits a 1-isometric completely protectable code $\mathcal{C}'_\mathcal{Q}$, and it admits a 1-isometric completely protectable code $\mathcal{C}'_\mathcal{Q}$ iff it admits a 1-isometric completely correctable code $\mathcal{C}''_\mathcal{Q}$.*

Proof. Clearly, if $\mathcal{C_Q}''$ is completely protectable it is also protectable. It then suffices to prove that the existence of a protectable code implies the existence of a completely correctable one, and this in turn implies the existence of a completely protectable one. Assume that $\mathcal{C}_\mathcal{Q}$, of the form given in Eq. (7), is protectable for $\mathcal{E}$, with a "protecting" quantum operation $\mathcal{R}$. Then, by the above argument, $\mathcal{C}_\mathcal{Q}$, $\mathcal{R}(\mathcal{C}_\mathcal{Q})$, and $\mathcal{E}\circ\mathcal{R}(\mathcal{C}_\mathcal{Q})$ must be 1-isometric state encodings of $\mathcal{Q}$ in $\mathcal{P}$ of the subsystem form. Let $\mathcal{C}'_\mathcal{Q} = \mathcal{R}(\mathcal{C}_\mathcal{Q})$. Then $\mathcal{C}'$ is preserved by $\mathcal{E}$, hence completely correctable by the previous Theorem.

Conversely, assume then that $\mathcal{C}'_\mathcal{Q}$ is completely correctable for $\mathcal{E}$, with correction operation $\mathcal{R}'$. Let $\mathcal{C}''_\mathcal{Q} = \mathcal{E}(\mathcal{C}'_\mathcal{Q})$. Then we have

$$(\mathcal{E}\circ\mathcal{R}')(\mathcal{C}''_\mathcal{Q}) = \mathcal{E}(\mathcal{C}'_\mathcal{Q}) = \mathcal{C}''_\mathcal{Q},$$

which is completely protectable. □

The role of isometries for 1-isometric subsystem encodings is illustrated in Figure 1. Note that while Theorem 4 above may be regarded as a direct counterpart of Theorem 1 in Ref. 10, the isometric approach has the advantage of additionally providing the explicit structure of the encoding, along with the explicit noise action and the required correction map. Furthermore, Corollary 1 formally establishes how protectable 1-isometric encodings are in fact equivalent to correctable ones. Intuitively, at least as far as perfect information recovery is concerned, we cannot hope to find a protectable code if no correctable codes of the same dimension are available.

Next, we consider the potential of unitary correction superoperators for 1-isometric codes. Our main result shows that unitary recovery may suffice, provided that the code is not increasingly "smeared" under the noise action, in the following sense:

Proposition 1 *Let $\mathcal{C}_\mathcal{Q}$ be a preserved 1-isometric code for $\mathcal{E}$, with* $\dim(\mathrm{supp}(\mathcal{E}(\mathcal{C}_\mathcal{Q}))) \le \dim(\mathrm{supp}(\mathcal{C}_\mathcal{Q}))$. *Then $\mathcal{C}_\mathcal{Q}$ is unitarily correctable.*

Proof. Consider a 1-isometric code $\mathcal{C}_\mathcal{Q}$ associated to $\mathcal{H}_S\otimes\mathcal{H}_F\oplus\mathcal{H}_R$ and preserved by $\mathcal{E}$. Thus, there exists a minimal Hilbert space decomposition $\mathcal{H}_{S'}\otimes\mathcal{H}_G\oplus\mathcal{H}_T$ associated to $\mathcal{E}(\mathcal{C}_\mathcal{Q})$, with $\dim(\mathcal{H}_S) = \dim(\mathcal{H}_{S'})$. If $\dim(\mathcal{H}_G) < \dim(\mathcal{H}_F)$, we may extend the decomposition to an non-minimal one $\mathcal{H}_{S'}\otimes\mathcal{H}_{G'}\oplus\mathcal{H}_{T'}$, in such a way that equality holds. Having ensured that $\dim(\mathcal{H}_{G'}) = \dim(\mathcal{H}_F)$, the two subsystem representations are isomorphic, and there exists a unitary correction superoperator $\mathcal{U}(\cdot) = U(\cdot)U^\dagger$ that restores the initial state up to the cofactor, which has rank at most equal to the initial one. Thus, Theorem 2 applies to $\mathcal{U}\circ\mathcal{E}$, and the code is supported on a NS for $\mathcal{U}\circ\mathcal{E}$. Therefore, it is unitarily correctable. □

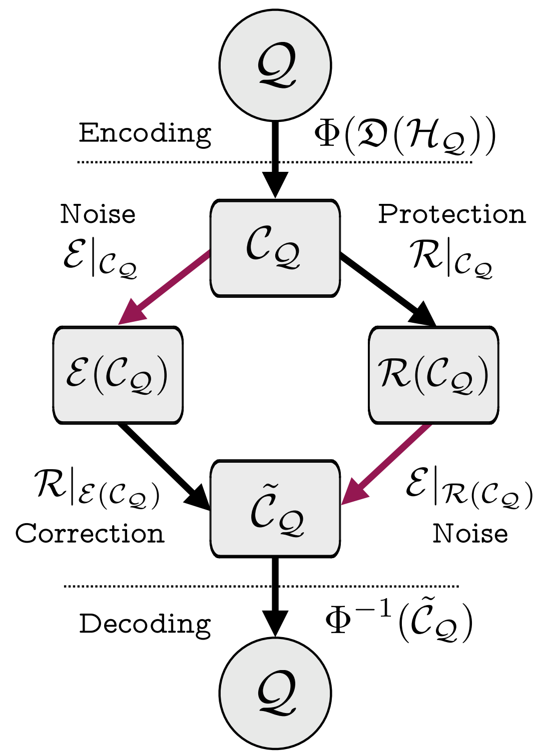

FIG. 1: (Color online) Pictorial representation of trace-norm isometries in quantum information encoding, correction, and protection. Here, $\tilde{\mathcal{C}}_Q$ denotes a code isomorphic to $\mathcal{C}_Q$, whereas the (state-)decoding map returns information from the physical back to the abstract level.

When the main assumption of the above Theorem is violated, that is, $\dim(\mathrm{supp}(\mathcal{E}(\mathcal{C}_\mathcal{Q}))) \le \dim(\mathrm{supp}(\mathcal{C}_\mathcal{Q}))$, we can still gain some insight on what can be achieved by restricting to unitary corrections: If, in the previous proof, $\dim(\mathcal{H}_G) > \dim(\mathcal{H}_F)$, we can define a non-minimal subsystem encoding for $\mathcal{C}_\mathcal{Q}$ such that $\dim(\mathcal{H}_G) = \dim(\mathcal{H}_F)$. Then there exists a unitary change of basis V such that $V(\rho\otimes\mathcal{E}_{\mathcal{F}'-\mathcal{G}'}(\tau'))V^\dagger$ is a 1-isometric encoding for $\mathcal{Q}$ in $\mathcal{H}_S\otimes\mathcal{H}_{F'}\oplus\mathcal{H}_{R'}$, equivalent to the initial subsystem decomposition. Since the support of $\mathcal{C}_\mathcal{Q}$ is strictly contained in $\mathcal{E}(\mathcal{C}_\mathcal{Q})$, Theorem 2 does not apply. This means that every 1-isometric subsystem encoding which is correctable is in general only *unitarily recoverable*, that is, there exists a unitary operation that restores the code to one which is supported by a non-minimal extension of the initial subsystem decomposition. This is weaker than the code being unitarily correctable, since there is *no* guarantee that further iterations of noise and correction will still preserve the code. We have thus recovered Theorem 1 in Ref. 15 (stating the equivalence between correctable and unitarily recoverable subsystems) as a corollary of our isometry-based analysis. An interesting open question for further investigation is to what extent direct connections might exist between with the characterization of unitarily correctable codes from the multiplicative domain of CPTP maps as recently pursued in [16]. Within the current analysis, we conclude our discussion on perfect isometric encodings by considering a simple illustrative example.

Example 1: The 3-bit quantum repetition code revisited. Consider a system of three qubits, described in $\mathcal{H}_\mathcal{P} \approx (\mathbb{C}^2)^{\otimes 3}$ with the standard computational basis $\{|abc\rangle = |a\rangle \otimes |b\rangle \otimes |c\rangle \,|_{\,a,b,c\in\{0,1\}}\}$. Assume that the dominant noise on the system stems from independent bit-flip errors with probability $p < 1/2$, that is, $\mathcal{E} \sim \{\sqrt{1-p}\,\sigma_0^{(i)}, \sqrt{\frac{p}{3}}\,\sigma_x^{(i)}\}_{i=1,2,3}$, where $\sigma_x^{(i)}$ are Pauli operators on the i-th qubit, and $\sigma_0^{(i)} = I$ corresponds to no-error. Consider the subspace $\mathcal{H}_\mathcal{C} = \mathrm{span}\{|000\rangle, |111\rangle\}$, which is used to encode the states of a logical qubit $\mathcal{Q}$, that is, in our notation, $\mathcal{C} = \mathcal{D}(\mathcal{H}_C)$. Let us consider the subsystem decomposition $\mathcal{H}_\mathcal{P} \sim \mathcal{H}_\mathcal{Q} \otimes \mathcal{H}_F$, induced by the unitary change of basis U defined by

$$U|abc\rangle = |x\rangle \otimes |yz\rangle, \tag{15}$$

where x is the majority count of the binary string abc, and yz indicates in which location abc differs from xxx, with 00 indicating no differences. Then, in the subsystem representation defined by Eq. (15), $\mathcal{H}_\mathcal{C} \sim \mathcal{H}_\mathcal{Q} \otimes |00\rangle$, $\mathcal{C} = \{\rho \otimes |00\rangle\langle 00|\}$, with $\rho \in \mathcal{D}(\mathcal{H}_\mathcal{Q})$, see also [1]. It is easy to see that the action of $\mathcal{E}$ *restricted to* $\mathcal{C}$ in this representation is $\mathcal{E}|_\mathcal{C} = I \otimes \mathcal{F}$, where explicitly

$$\begin{aligned}\mathcal{F}(|00\rangle\langle 00|) \equiv \sigma &= (1-p)|00\rangle\langle 00| \\ &+ \frac{p}{3}(|01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|).\end{aligned}$$

Thus, $\mathcal{E}(\mathcal{C}) = \{\rho \otimes \sigma\}$ is 1-isometric to $\mathcal{C}$. By using a correction superoperator $\mathcal{R} = I \otimes \mathcal{A}$, where for instance $\mathcal{A}$ is a two-qubit amplitude damping channel on $\mathcal{H}_F$ (such that for any σ, $\mathcal{A}(\sigma) = |00\rangle\langle 00|$), it follows that $\mathcal{C}$ is fixed for $\mathcal{R} \circ \mathcal{E}$. Equivalently, $\mathcal{H}_\mathcal{C}$ is a DFS under $\mathcal{R} \circ \mathcal{E}$. On the other hand, one may directly verify that the code $\mathcal{C}' \equiv \mathcal{E}(\mathcal{C})$ is completely protectable for $\mathcal{E}$, with protection operation $\mathcal{R}$ as above, as it follows from the proof of Corollary 1. Equivalently, $\mathcal{H}_\mathcal{Q}$ supports a NS of $\mathcal{E} \circ \mathcal{R}$.

While the fact that *every* (finite-distance) subspace QEC code is associated to a NS of $\mathcal{E} \circ \mathcal{R}$ is implied by Theorem 6 in [2], OQEC subsystem codes take explicit advantage of the fact that a NS may also be identified for $\mathcal{R} \circ \mathcal{E}$, for the same $\mathcal{R}$, see [32] for the simplest representative of an OQEC code which protects one logical qubit into nine qubits subject to arbitrary independent single-qubit errors.

IV. ROBUSTNESS OF ISOMETRIC ENCODINGS

The 1-isometric setting we analyzed thus far naturally lends itself to investigate robustness properties of subsystem encodings. In turn, this allows to place our approach in the context of approximate QEC, which has been extensively investigated for subspace codes from different perspectives (see *e.g.* [33, 35, 36, 37, 38]), and is now receiving renewed attention in the light of extensions to the more general case of OQEC and subsystem codes [18, 19, 20]. While a comprehensive study is beyond our current scope, we focus here on two representative kinds of uncertainty sources:

- *Encoding uncertainty:* The procedure that implements the intended encoding map may be affected by errors.
- *Model uncertainty:* The noise model for which the code and correction operator are intended may be only approximately known.

For 1-isometric encodings as defined in Sec. I, we show here that error correction is robust with respect to bounded encoding errors. Furthermore, an upper bound may be given on how information is degraded in the presence of modeling errors. The key idea is to invoke perturbations of 1-isometries:

Definition 4 *A map $\tilde{\Phi} : \mathcal{O}(\mathcal{H}_\mathcal{A}) \to \mathcal{O}(\mathcal{H}_\mathcal{B})$ is a perturbation of a 1-isometry if there exist a 1-isometry $\Phi : \mathcal{O}(\mathcal{H}_\mathcal{A}) \to \mathcal{O}(\mathcal{H}_\mathcal{B})$ and $\varepsilon \in \mathbb{R}^+$ such that*

$$\|\tilde{\Phi}(\rho) - \Phi(\rho)\|_1 \leq \varepsilon, \quad \forall \rho \in \mathcal{D}(\mathcal{H}_\mathcal{Q}).$$

Approximate isometries on Banach spaces have been introduced by Hyers and Ulam in the 40's [39] in their most general form [40], and since then their properties have been studied intensively, most notably approximations with linear or affine isometries as well as various extension problems, see *e.g.* [41, 42, 43, 44] and references therein. Note that in our context we consider only approximate isometries that are *ε-perturbations of linear 1-isometries* and, for the sake of brevity, we still refer to them simply as ε-isometries. The definitions of approximate 1-isometric encodings and of approximately preserved codes are then the natural extension of the exact ones to this setting. In particular:

Definition 5 *A state encoding $\tilde{\Phi}$ of $\mathcal{Q}$ in $\mathcal{P}$ is an ε-isometric encoding if $\tilde{\Phi}$ is a ε-isometry.*

It follows from our previous analysis that ε-isometric state encodings have the following structure:

$$\tilde{\Phi}(\rho) = \rho \otimes \tau \oplus \hat{0}_R + \Delta(\rho), \tag{16}$$

with $\|\Delta(\rho)\|_1 \leq \varepsilon$. In this way, given the properties of the trace-norm, and the relation of the latter to distinguishability, the perturbation parameter ε inherits the role of an *upper bound* to the error probability in information recovery via measurements. The other relevant definitions are also extended in a similar fashion:

Definition 6 *A code $\mathcal{C}_Q$ is (i) ε-*preserved *for $\mathcal{E}$ if $\mathcal{E}|_{\mathcal{C}_Q}$ is a ε-isometry; (ii) ε-*noiseless *for $\mathcal{E}$ it is ε-preserved for any convex combination of the form $\sum_k p_k \mathcal{E}^k$; (iii) ε-*correctable *if it is ε-noiseless for $\mathcal{R}\circ\mathcal{E}$.*

A. Encoding uncertainty

The correction operations for 1-isometric codes we discussed in Sec. III.B exhibit a desirable property: Bounded errors in the encoding map do not increase. This is formalized by the following:

Proposition 2 *Let Φ be a 1-isometric encoding such that its range $\mathcal{C}_Q$ is preserved by $\mathcal{E}$. Then any ε-approximate version $\tilde{\Phi}$ generates ε-approximate codes $\tilde{\mathcal{C}}_Q$ which are ε-correctable for $\mathcal{E}$.*

Proof. Under the assumptions, any $\tilde{\mathcal{C}}_Q$ is of the form

$$\tilde{\Phi}(\rho) = \rho\otimes\tau\oplus\hat{0}_R + \Delta(\rho),$$

with $\|\Delta(\rho)\|_1 \le \varepsilon$ and $\rho\otimes\tau\oplus\hat{0}_R \in \mathcal{C}_Q$, which is preserved hence completely correctable. Let $\mathcal{R}$ be the TPCP map that implements the complete correction, and let $\bar{\mathcal{E}}_p = \sum_j p_j(\mathcal{R}\circ\mathcal{E})^j$ be any convex combination. Then

$$\bar{\mathcal{E}}(\rho\otimes\tau\oplus\hat{0}_R + \Delta(\rho)) = \rho\otimes\tau\oplus\hat{0}_R + \bar{\mathcal{E}}(\Delta(\rho)).$$

Given that $\sum_j p_j(\mathcal{R}\circ\mathcal{E})^j$ is a trace-norm contraction, it follows that $|\sum_j p_j(\mathcal{R}\circ\mathcal{E})^j(\Delta(\rho))| \le \varepsilon$. □

B. Model uncertainty

Errors due to model uncertainty may cause the encoded information to degrade rapidly: In fact, monotonicity of the trace norm under CPTP dynamics is not enough to ensure non-increasing errors as in Section IV A. We provide a bound on the norm-1 error after a finite number of iterations of an approximately preserved code.

Since $\mathcal{C}_Q$ is ε-approximately preserved, there exists a subsystem decomposition such that for every $\rho\in\mathcal{D}(\mathcal{H}_Q)$, we may write

$$(\mathcal{E}\circ\Phi)(\rho) = \rho\otimes\tau\oplus\hat{0}_R + \Delta(\rho),$$

with $\|\Delta(\rho)\|_1 \le \varepsilon$ and $\mathcal{E}'|_{\mathcal{C}_Q} = \mathcal{E} - \Delta$ being a 1-isometry. Choose $\mathcal{R}$ such that $\mathcal{C}_Q$ is fixed for $\mathcal{R}\circ\mathcal{E}'|_{\mathcal{C}_Q}$, as invoked in the proof of the previous Proposition. Therefore,

$$(\mathcal{R}\circ\mathcal{E})^n(\rho) = \rho + \mathcal{R}\left(\sum_{i=1}^{n}(\mathcal{E}\circ\mathcal{R})^{i-1}(\Delta(\rho))\right), \quad (17)$$

where now $\rho\in\mathcal{C}_Q$. By recalling that both $\mathcal{R}$ and $\mathcal{E}\circ\mathcal{R}$ act as a trace-norm contraction, it follows that for any i,

$$\|\mathcal{R}\circ(\mathcal{E}\circ\mathcal{R})^i(|\Delta(\rho))\|_1 \le \|(\mathcal{E}\circ\mathcal{R})^i(\Delta(\rho))\|_1 \le \varepsilon.$$

We thus have the following:

Proposition 3 *Any ε-preserved code $\mathcal{C}_Q$ under $\mathcal{E}$ admits a correction operation $\mathcal{R}$ such that $\mathcal{C}_Q$ is $\tilde{\varepsilon}$-preserved by $(\mathcal{R}\circ\mathcal{E})^n$, with $\tilde{\varepsilon}\le n\varepsilon$.*

While it is possible to construct instances in which equality holds (at least for low n), an interesting question is whether the bound can be tightened under additional information on $\Delta(\rho)$. Suppose, for instance, that $\mathcal{E}\circ\mathcal{R}$ is *strictly contractive* along any trajectory $\mathcal{T}_\rho = \{(\mathcal{R}\circ\mathcal{E})^i(\Delta(\rho));\, i\in\mathbb{N}\}$, $\rho\in\mathcal{C}_Q$, that is, there exists an $\alpha\in[0,1)$ (possibly dependent upon ε) such that $\|\mathcal{E}\circ\mathcal{R}(X)\|_1 \le \alpha\|X\|_1$, $\forall X\in\mathcal{T}_\rho$. Under these assumptions, given Eq. (17), the relevant bound becomes a geometric sum, and there exists a value

$$\tilde{\varepsilon} \le \lim_{n\to\infty}\sum_{i=1}^{n}\alpha^{i-1}\varepsilon = \frac{\varepsilon}{1-\alpha},$$

so that the code is $\tilde{\varepsilon}$-correctable. The fact that the set of strictly contractive maps is dense in the set of all CPTP maps [45] leaves in principle the door open for approximate long-term information preservation in a generic setting. In practice, whether the error bound is acceptable for the intended application has be tested on a case-by-case basis. We again provide an illustrative example.

Example 2: The approximate 3-bit quantum repetition code. Consider the same two-qubit system and the same code described in Example 1, but assume now that the error model is described by

$$\mathcal{E}_\varepsilon = (1-\varepsilon)\mathcal{E} + \varepsilon\,\mathcal{G}, \quad 0<\varepsilon<1,$$

with $\mathcal{E}$ accounting for independent bit-flip errors as in Example 1, and $\mathcal{G}$ for independent phase-flip errors. That is, $\mathcal{G}\sim\{\sqrt{1-p}\,\sigma_0^{(i)}, \sqrt{\frac{p}{3}}\,\sigma_z^{(i)}\}_{i=1,2,3}$, where as before $\sigma_z^{(i)}$ acts on the i-th qubit, and $\sigma_0^{(i)} = I$.

Assume that we are interested in testing how well the corrected code performs after a given number of iterations of errors followed by recovery, where $\mathcal{R}$ is chosen in the perfect case. For concreteness, we let $n = 10$, $\varepsilon = 0.050$, and $p = 0.4$ for both $\mathcal{E}$ and $\mathcal{G}$. The linear bound of Proposition 3 predicts that the error in trace norm should be at most $\bar{\varepsilon} = 0.5$. Since states represented by matrices diagonal in the computational basis are clearly unaffected by the addition of a dephasing term like $\mathcal{G}$, we choose as a test encoded state

$$\rho_c = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}.$$

After 10 iterations, the recovered state reads

$$\rho_{10} = \begin{pmatrix}0.500 & 0.332\\ 0.332 & 0.500\end{pmatrix},$$

which leads to the following error in trace distance:

$$\varepsilon_{10} = \text{trace}(|\rho_c - \rho_{10}|) = 0.335.$$

It is easy to show that asymptotically the encoded qubit undergoes a complete dephasing process. That is, for any initial encoded state ρ_0, we get:

$$\lim_{n\to\infty}(\mathcal{R}\circ\mathcal{E})^n(\rho_0) = \lim_{n\to\infty}(\mathcal{R}\circ\mathcal{E})^n \begin{pmatrix} a & b \\ b^* & c \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}.$$

Using a state like ρ_c, the asymptotic error thus becomes $\varepsilon \to 1$, rendering this approximate code unfit for use whenever a large number of iteration is needed.

V. CONCLUSIONS

We have shown that trace-norm isometries provide an operationally motivated and mathematically consistent framework for addressing encoding and preservation of quantum information in physical systems. Our results point to a number of possible extensions and open problems, some of which have been already highlighted in the main text. A first natural step is motivated by considering information protection and correction in the Heisenberg picture, which calls for a constructive characterization of observable encodings in relation to the general subsystem structure of state encodings obtained in Sec. I. From a general QEC standpoint, two interesting problems arise from seeking extensions of the present 1-isometric framework that may be applicable to continuous-time (Markovian) dynamics and OQEC [46], or that relax the correctability notion to allow for non-CP transformations [47] (Markovian) dynamics [46]. Since the basic mathematical result on which our treatment relied (Busch's Theorem, from Ref. 25) applies to arbitrary separable Hilbert spaces in its full generality, extensions to infinite-dimensional settings and quantum information with continuous variables are also conceivable in principle. Lastly, the problem of detecting when a map is "close" to an isometry (with respect to the standard Hilbert-space inner product) has recently been shown to be `QMA`-hard [48]. It is suggestive to speculate that analogous complexity results for trace-norm isometries might allow to further characterize the complexity of finding preserved quantum codes `NP`-hard [10, 11].

Acknowledgments

We are indebted to Lajos Molnar for relevant references from the mathematical physics literature. F.T. acknowledges hospitality from the Physics and Astronomy Department at Dartmouth College, where this work was performed, and support from the University of Padova under the QUINTET project of the Department of Information Engineering, and the QFUTURE and CPDA080209/08 research grants. L.V. gratefully acknowledges partial support from the NSF under grant No. PHY05-51164.

[1] L. Viola, E. Knill, and R. Laflamme, J. Phys. A **34**, 7067 (2001).

[2] E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000).

[3] L. Viola and E. Knill, Phys. Rev. A **68**, 032311 (2003).

[4] E. Knill, Phys. Rev. A **74**, 042301 (2006).

[5] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).

[6] D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1997).

[7] D. W. Kribs, R. Laflamme, and D. Poulin, Phys. Rev. Lett. **94**, 180501 (2005).

[8] D. W. Kribs, R. Laflamme, D. Poulin, and M. Lesosky, Quantum Inf. Comput. **6**, 382 (2006).

[9] T. Brun, I. Devetak, and M. H. Hsieh, Science **314**, 436 (2006).

[10] R. Blume-Kohout, H. K. Ng, D. Poulin, and L. Viola, Phys. Rev. Lett. **100**, 030501 (2008).

[11] R. Blume-Kohout, H. K. Ng, D. Poulin, and L. Viola, in preparation (2009).

[12] C. A. Fuchs and J. van de Graaf, IEEE Trans. Inf. Theory **45**, 1216 (1999).

[13] D. A. Lidar, P. Zanardi, and K. Khodjasteh, Phys. Rev. A **78**, 012308 (2008).

[14] K. Khodjasteh, D. A. Lidar, and L. Viola, arXiv: 0908.1526 (2009).

[15] D. W. Kribs and R. W. Spekkens, Phys. Rev. A **74**, 042329 (2006).

[16] M.-D. Choi, N. Johnston, and D. W. Kribs, J Phys. A **42**, 245303 (2009).

[17] B. Schumacher and M. D. Westmoreland, J. Math. Phys. **50**, 032106 (2009).

[18] C. Bény and O. Oreshkov, arXiv:0907.5391 (2009).

[19] C. Bény, arXiv:0907.4207 (2009).

[20] H. K. Ng and P. Mandayam, arXiv:0909.0931 (2009).

[21] Note that the domain of Φ is extended to arbitrary positive semidefinite operators by defining: $\Phi(\Pi_A^\lambda \rho \Pi_A^\lambda) = \text{trace}(\Pi_A^\lambda \rho)\Phi\left(\Pi_A^\lambda \rho \Pi_A^\lambda / \text{trace}(\Pi_A^\lambda \rho)\right)$.

[22] A. Holevo, *Statistical Structure of Quantum Theory*, Lecture Notes in Physics; Monographs: **67** (Springer-Verlag, Berlin, 2001).

[23] D. Petz, *Quantum Information Theory and Quantum Statistics* (Springer-Verlag, Berlin Heidelberg, 2008).

[24] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Information* (Cambridge University Press, Cambridge, 2002).

[25] P. Busch, Math. Phys. Anal. Geom. **2**, 83 (1999).

[26] L. Molnar and W. Timmermann, J. Phys. A **36**, 267 (2003).

[27] A related result by P. Mankiewicz [Thm. 5 in Bull. Acad. Polon. Sciences **20**, 367 (1972)] states that any bijective isometry between convex sets with *nonempty interiors*

can be uniquely extended to a bijective affine isometry between the whole spaces. Note that a direct application of this result to 1-isometric (not necessarily linear) encodings defined on density $\mathcal{D}(\mathcal{H}_Q)$) is prevented by the fact that the image $\Phi(\mathcal{D}(\mathcal{H}_Q))$ need not have nonempty interior in general.

[28] In principle, different choices of observable encodings may be considered. For example, I_F may be substituted by a different fixed operator X_F, even if in that case some of the faithfulness requirements may need reconsideration as they may fail. In practice, beside being directly suggested by the results on faithful encodings, the choice of I_F on $\mathcal{H}_F$ is particularly convenient, as it also ensures robustness with respect to the co-factor state (see Sec. III A). Also, the choice of X_R could in principle depend on A, but it would nevertheless remain irrelevant with respect to the faithfulness requirements, given the form of an isometric encoding.

[29] D. Kribs, R. Laflamme, and D. Poulin, Phys. Rev. Lett. **94**, 180501 (2005).

[30] G. Lindblad, Lett. Math. Phys. **47**, 189 (1999).

[31] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).

[32] D. Bacon, Phys. Rev. A **73**, 012340 (2006).

[33] H. Barnum and E. Knill, J. Math. Phys **43**, 2097 (2002).

[34] F. Ticozzi and M. Pavon, arXiv:0811.0929 (2008).

[35] B. Schumacher and M. D. Westmoreland, Quantum Inf. Process. **1**, 5 (2002).

[36] R. Klesse, Phys. Rev. A **75**, 062315 (2007).

[37] F. Buscemi, Phys. Rev. A **77**, 012309 (2008).

[38] D. W. Leung, M. A. Nielsen, I. L. Chuang, and Y. Yamamoto, Phys. Rev. A **56**, 2567 (1997).

[39] D. H. Hyers and S. M. Ulam, Bull. Am. Math. Soc. **51**, 288 (1945).

[40] Let $\mathcal{A}, \mathcal{B}$ be Banach spaces. A map $f : \mathcal{A} \to \mathcal{B}$ is an *ε-isometry* if for every $x, y \in \mathcal{A}$ it obeys $|\|f(x) - f(y)\| - \|x - y\|| \leq \varepsilon$, for some $\varepsilon \in \mathbb{R}^+$.

[41] R. Bhatia and P. Semrl, Am. Math. Month. **104**, 497 (1997).

[42] S. J. Dilworth, Bull. Lon. Math. Soc. **31**, 471 (1999).

[43] T. Rassias, Internat. J. Math. Math. Sci **25**, 73 (2001).

[44] R. Liu and L. Zhang, J. Math. Anal. App. **352**, 749 (2009).

[45] M. Raginsky, Phys. Rev. A **65**, 032306 (2002).

[46] O. Oreshkov, D. A. Lidar, and T. Brun, arXiv:0806.3145 (2008).

[47] A. Shabani and D. A. Lidar, Phys. Rev. A **80**, 012309 (2009).

[48] B. Rosgen, arXiv:0910.3740 (2009).